(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification[7]: **H04L 9/00**

(21) International Application Number: PCT/US02/02218

(22) International Filing Date: 24 January 2002 (24.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/770,525   25 January 2001 (25.01.2001)   US

(71) Applicant *(for all designated States except US)*: **SOLU-TIONARY, INC.** [US/US]; 9420 Underwood Avenue, Omaha , NE 68114 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **HRABIK, Michael** [US/US]; 9420 Underwood Avenue, Omaha, NE 68114 (US). **GUILFOYLE, Jeffrey** [US/US]; 9420 Underwood Avenue, Omaha, NE 68114 (US). **BEAVER, Edward, Mac** [US/US]; 9420 Underwood Avenue, Omaha, NE 68114 (US).

(74) Agent: **ANGOTTI, Donna, L.**; Schulte Roth & Zabel, LLP, 919 Third Avenue, New York, NY 10022 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Published:
— with international search report
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR VERIFYING THE INTEGRITY OF COMPUTER NETWORKS AND IMPLEMENTATION OF COUNTER MEASURES
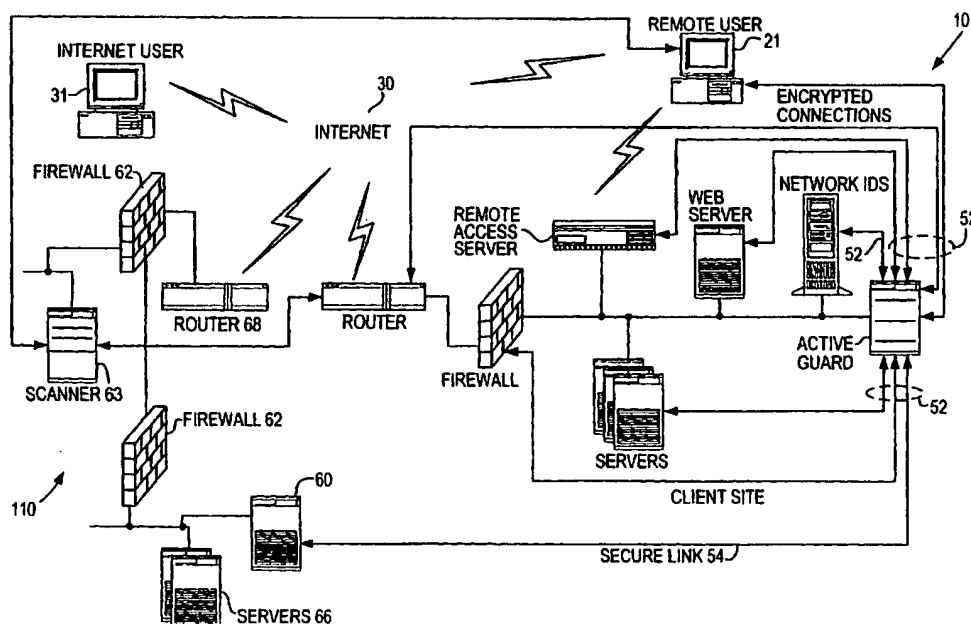
(57) Abstract: A method and apparatus for verifying the integrity of devices on a target network (100) having two components: a subsystem (50) connected to the target network (100), and a master system (60), isolated therefrom by a secure lin (52). The topological and hierarchical relationship of the devices to each other improves stability of the apparatus. Random testing of the subsystem (50) by the master system (60) provide verification and independent self-checking.

METHOD AND APPARATUS FOR VERIFYING THE INTEGRITY OF COMPUTER NETWORKS AND IMPLEMENTATION OF COUNTER MEASURES

FIELD OF THE INVENTION

This invention relates to a method and apparatus for verifying the integrity of a computer security subsystem for preventing attacks on computer network security systems.

BACKGROUND OF THE INVENTION

Concurrent with the rise in connectivity among diverse computer networks and the corresponding increase in dependence on networked information systems, there has been a dramatic increase in the need for robust security to enforce restrictions on access to and prevent intrusion on secure systems. The topology of the interconnected networks has also grown increasingly complex, and often involves open networks such as the internet that expose secure systems to increased threats of attack. Consequently, no single solution has yet been proposed that addresses all current needs for intrusion detection and response. Instead, a vast assortment of security devices and techniques has evolved and has generally been implemented differently on individual systems. This has resulted in a global security patchwork, inherently susceptible to attack and to individual systems which themselves implement a hodge podge of different security devices and techniques.

Attempts to gain unauthorized access to computer networks capitalize on inherent loopholes in a network's security topology. It is known, for example, that although a secure system connected to the internet may include firewalls and intrusion detection systems to prevent unauthorized access, weaknesses in individual security components are often sought out and successfully exploited. The rapid introduction of new technology exacerbates the problem, creating or exposing additional weaknesses that may not become known until a breach in security has already occurred.

A fundamental weakness shared in common by current intrusion detection and response systems is their "flat" or non-hierarchical implementation. The configuration shown in Fig. 1 is an example of such a typical network implementation on a hypothetical "target network." The network 10 includes a plurality of file servers 14, workstations 16, a network intrusion detection system (IDS) 18, a remote access server 20 and a web server 22. These devices are connected to each other over network backbone 12, and form a local or wide-area network (LAN or WAN). Router 26 is connected directly to an open network such as the internet, 30, and is connected to the devices on network backbone 12 through network firewall 24.

The firewall 24 and the IDS 18 are part of the security system of network 10. Firewall 24 is configurable and serves to control access by hosts on the internet to resources on the network. This protects network 10 from intruders outside the firewall, essentially by filtering them out. IDS 18 scans packets of information transmitted over backbone 12 and is configured to detect specific kinds of transactions that indicate that an intruder is attempting, or already has gained access to the network, 10. In this way, the IDS protects the network from intruders inside as well as outside the firewall. Other devices on network 10 may also contribute to network security, such as remote access server 20 which permits access directly to network 10 from remote computers (not shown), for example, over a modem. Remote access server 20 must also implement some security function such as username and password verification to prevent intruders from gaining access to the network and bypassing firewall 24.

In a typical intrusion scenario on a target network connected to the internet, an intruder will first learn as much as possible about the target network from available public information. At this stage, the intruder may do a "whois" lookup, or research DNS tables or public web sites associated with the target. Then, the intruder will engage in a variety of

2

common techniques to scan for information. The intruder may do a "ping" sweep in order to
see which machines on the target network are running, or they may employ various scanning
utilities well known in the art such as "rcpinfo", "showmount" or "snmpwalk" to uncover
more detailed information about the target network's topology. At this stage the intruder has
done no harm to the system, but a correctly configured network IDS should be able,
depending on its vantage point on the network, to detect and report surveillance techniques of
intruders that follow known patterns of suspicious activitity. These static definitions, known
as "intrusion signatures", are effective only when the intruder takes an action or series of
actions that closely follow the established definitions of suspicious activity. Consequently, if
the IDS is not updated, is disable or encounters an unknown or new method of attack, it will
not respond properly. However, if steps are not taken at this point in the attack to prevent
further penetration into the target network, the intruder may actually begin to invade the
network, exploiting any security weaknesses (such as the IDS that may have not reacted
earlier to the intruder), and securing a foothold on the network. Once entrenched, the intruder
may be able to modify or disable any device belonging to the target network including any
remaining IDS or firewall.

    Methods used by intruders to gain unauthorized access to computer networks
evolve in sophistication in lock step with advances in security technology. It is typical,
however, that successful attacks on network systems often begin by attacking the security
subsystems in place on the target network that are responsible for detecting common
intrusion signatures, disabling those systems and destroying evidence of the intrusion.

    U.S. Patent No. 5,916,644 to Kurtzberg et al. discloses a method for testing
the integrity of security subsystems wherein a specifically configured system connected
directly a target computer network will systematically test security on the network by
simulating attacks on security devices in order to verify that they are operational.

Specifically, the disclosed method randomly simulates an attack on the network. If the attack

is detected, the security subsystems are assumed to be functioning. If not, they are

considered compromised, and an attack may already be underway. This method is an

improvement over passive systems that do not check themselves and therefore cannot

properly report on their own status when they have been disabled.

A major shortcoming of this approach is that these security systems reside on

the same networks that they seek to protect and are similarly vulnerable to attack once an

intruder has gotten a foothold on the network. In other words, they are not themselves

immune to the attacks of intruders. As a result each advance in the prior art is just another

new security hurdle on the network to be defeated. In this light, the active scanning approach

disclosed in Kurtzberg is not fundamentally different from any other security measure (such

as firewall) in that it is non-hierarchical and depends completely on the vigilance of a human

network manager.

Therefore, there exists a need for self-diagnosing network security system that

can protect a target network from both internal and external intruders and that is resistant to

attacks perpetuated on the system it has been deployed to protect. Furthermore, there is a

need for an active security system that will take measured action against perceived security

threats even in the absence of a human network manager.

Summary of the Invention

It is therefore an object of the present invention to provide a network security

system for a network of computers that is capable of solving the above mentioned problems

in the prior art.

It is another object of the present invention to provide a network security

system that has a component that can directly monitor multiple network security devices on a

4

network for attack signatures and other suspicious network activity suggesting an attempt to compromise security on that network.

It is another object of the present invention to provide a network security system that can dynamically detect new patterns or trends in network activity that suggests an attempt to compromise network security on a single network or on a plurality of otherwise unrelated networks.

It is another object of the present invention to provide a network security system that can resist intrusion during an attack on the network.

It is another object of the present invention to provide a security system providing integrity verification for security devices on a network, and can also reliably verify its own integrity.

It is another object of the present invention to provide a security system for a computer network that can take corrective measures after an attack has been detected to prevent an intruder from gaining further access to the network.

It is another object of the present invention to provide a security system satisfying the above objectives for individual computers connected to an open network.

According to an example of the present invention, there is provided a network security system to prevent intrusion on a target network having at least one security subsystem local to the target network provided to monitor network traffic an to detect attacks by an intruder on the system. The subsystem is connected via a secure link to a master system that is not otherwise connected to the target system. The master system monitors the subsystem via the secure link and registers information pertaining to the status of the subsystem. If the subsystem detects an attack on the target network, or does not respond to the master system, the master system will take appropriate action, ranging from logging the incident or notifying a network manager to attempting to shut down the network.

Accordingly, even attacks that completely disable the subsystem will not prevent the master system from responding as long as the link remains secure.

According to another example of the present invention, a multi-level hierarchy is implemented making the subsystem subordinate to the master system. In this configuration, commands can only be passed from the master system to the subsystem, ensuring that the integrity of the master system can not be undermined, even if by successful attacks on the target network, or on the subsystem itself. Therefore, even a subversion of the subsystem and a compromised link between it and the master system is insufficient to disable the master system.

According to another example of the present invention, a pseudo-attack generator associated with the master system is provided that simulates attacks on the target network that should be directed by the subsystem. By comparing the pseudo-attacks made on the target network to the attacks actually detected by the subsystem, the master system can determine whether the integrity of the subsystem has been compromised. Similarly, the subsystem may generate its own pseudo-attacks on other network security components to establish their integrity as well. Therefore it is possible to test comprehensively every security-related device connected to the target network.

In another example of the present invention, the subsystem, and the master system acting through the subsystem, can implement corrective measures to mitigate or thwart suspected intruder attacks on the target network.

BRIEF DESCRIPTION OF THE DRAWINGS:

Fig. 1 is a block diagram showing the overall structure of an example of a network system according to the prior art.

Fig. 2 is a block diagram showing an example of a network incorporating the system of the present invention.

6

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiments of a network security system according to the present invention will hereinafter be described with reference to the accompanying drawings.

Referring to Fig. 2, a first embodiment of the present invention is shown. Target network 100 is shown having the same basic components as the network of the prior art shown in Fig. 1 with the addition of security subsystem 50, however it should be noted that the actual configuration of the target network is not critical with the exception of at least one security subsystem 50. Each of the security subsystem 50, servers 14, workstations 16, IDS 18, remote access server 20, web server 22, firewall 24 and router 26 are connected together over network backbone 12. Each of the devices carry out communication over the backbone in accordance with a predetermined communication protocol such as Transmission Control Protocol/Internet Protocol (TCP/IP).

Target network 100 is connected through firewall 24 and router 26 to the internet 30 as well as through remote access server 20 which may also be selectively connected to the internet 30 through remote user 21. These two potential points of contact with an open network, in this case the internet, exposes target network 100 to the threat of intrusion from any host with access to the internet such as internet user 31. In addition to threats from the outside, those with direct access to the resources of target network 100, such as those using one of the workstations 16, also pose an intrusion threat. If an intruder were to gain access to one of the critical security-related devices such as the IDS 18 or the firewall 24 or any trusted computer from within or outside the target network 100, security on the network could be compromised.

In the present invention, security subsystem 50 is connected to network backbone 12 and linked to each of the network's devices by a secure link 52. Such a secure link may be established through an encrypted communication protocol such as Secure

7

Sockets Layer (SSL). This ensures that communication between the security subsystem 50

and the other components of the target network cannot be intercepted by an intruder. A

similar secure link 54 is established as a virtual private network (VPN) tunnel between the

security subsystem 50 and a master system 60 connected to a remote network 110. Although

the remote network is shown having its own firewalls 62, servers 66, and router 68, the

ultimate configuration of remote network 110 is not critical beyond secure link 54 connecting

security subsystem 50 and master system 60. However, secure links 55 may be established

between a device such as a network scanner 63 and a router 26 or remote user 21 on network

100. Secure link 54 ensures that communication between the two networks cannot be

intercepted by an intruder. Therefore, there should be no other direct connection between

target network 100 and remote network 110 except over a secure link.

Preferably, the security system defined herein is embedded as a software

package and implemented on computers comprising at least a master system and the security

subsystem.

During operation, security subsystem 50 monitors the activities of the devices

of the target network 100. Particularly, the critical security-related functions of IDS 18 and

firewall 24 are tested. The particular method employed by security subsystem 50 in testing

these devices is not critical, however the above mentioned approach employing simulated

attacks on the components would be suitable.

Upon testing the devices, if the integrity of a device on target network 100

cannot be verified, security subsystem 50 reacts. For example, if IDS 18 has been identified

by the subsystem as not reacting properly to attacks on it originating from the internet,

appropriate countermeasures could include cutting off or restricting access to the network at

firewall 24 or stop at application level. If instead, the firewall is determined not to be

functioning, appropriate action might include disabling access to any servers 14 holding

sensitive date. In one possible configuration of the present invention, security subsystem 50 reports network device status to master system 60 which processes the information, and decides on further action. In an alternate configuration, security subsystem 50 is responsible for implementing countermeasures directly. In both cases, however, the results of every test are passed to master system 60 where they are stored for analysis.

The system of the present invention can also help thwart ongoing attacks and is uniquely suited to do so. In another preferred embodiment of the present invention, master system 60 hierarchically supercedes security subsystem 50. As such, the activities of security subsystem 50 are defined as a child process of master system 60 and are subordinate thereto. Although information preferably flows both ways between master system 60 and security subsystem 50 in this embodiment, the master system in this embodiment does not take direction from the subsystem.

As noted in the discussion of the prior art, non-hierarchical security systems are connected directly to a target network and are inherently susceptible to attacks on that network. This is in contrast to the present embodiment wherein, even if completely subverted during an attack on target system 100, security subsystem 50 would not result in a takeover of master system 60. The benefit of this configuration is that the master system would still be able to carry out its function. For example, if master system 60 is configured to sound an alarm when security subsystem 50 no longer responds to it, there would be no way, in this embodiment, for intruders on target network 100 to remotely shut down master system 60 because the master system will not respond to any instructions issued from a subordinate system. Although master system 60 may lose control of the target network, it is not in danger of being taken over by it. Additionally, if the link 54 between master system 60 and security subsystem 50 is severed or compromised, instructions may be routable instead through secure links 55.

9

In yet another embodiment of the present invention, remote network 110 is connected through router 70 to an open network such as the Internet. This enables master system 60 to send random pseudo-attacks to target network 100. The pseudo-attacks may mimic any of the actual attack signatures known by the master system to be detectable by the target network. If the expected reply is not received by the master system, an early indication of an intruder attack on the target network is indicated.

As set forth hereinabove, according to the present invention, it is possible to provide a method and apparatus for verifying the integrity of computers and computer networks that is independent of the network or computer being tested. In addition, by detecting early signs of intruder activity on a network, the present invention increases the likelihood that intruder attacks can be thwarted before they succeed.

When implemented on an individual computer, such as a single workstation 16 connected to an open network such as internet 30, the present invention functions similarly to prevent attacks on that computer originating from the open network. In the absence of network backbone 12 the functions of security subsystem 50 may be directly incorporated into an individual computer such as by software or peripheral hardware.

When implemented across a plurality of otherwise unrelated target networks, the present invention functions to prevent attacks according to the methods described herein on each target network individually. The advantage of this configuration is that security information may be coordinated across several networks without connecting the networks together.

Many different embodiments of the present invention may be constructed without departing from the sprit and scope of the invention. It should be understood that the present invention is not limited to the specific embodiments described in this specification.

10

To the contrary, the present invention is intended to cover various modifications and equivalent arrangements included within the spirit and the scope of the claims.

11

I claim:

1.   A security system for a computer connected to a network of computers comprising:

at least one security subsystem associated with said computer, said subsystem configured to detect attacks on said computer;

and a secure link between said security subsystem and a master system enabling data communication therebetween; wherein

said master system monitors said security subsystem through said secure link and registers information pertaining to attacks detected by said security subsystem.

2.   The security system of Claim 1 further comprising a pseudo attack generator associated with said master system for generating attacks on said computer detectable by said security subsystem wherein said master system monitors said security subsystem by comparing said pseudo-attacks to said attacks detected by the security subsystem.

3.   The security system of Claim 1 wherein said master system is hierarchically independent from said security subsystem.

4.   The security system of Claim 1 wherein said security subsystem is hierarchically subordinate to said master system.

5.   A network security system for a target network of computers comprising:

at least one security subsystem associated with said target network, said subsystem configured to detect attacks on said network; and

a secure link between said security subsystem and a master system enabling data communication therebetween; wherein

said master system monitors said security subsystem through said secure link and registers information pertaining to the attacks detected by said security subsystem.

6.   The network security system of Claim 5 wherein said master system is hierarchically independent from said security subsystem.

12

7.   The network security system of Claim 5 wherein said security subsystem is hierarchically subordinate to said master system.

8.   A network security system for a target network of computers comprising:

at least one security subsystem associated with said target network and configured to detect and register attacks on said target network;

a secure link for data communication between said security subsystem and said master system; and

testing means associated with said master system for generating pseudo-attacks on said target network initiated by said master system and detectable by said security subsystem; wherein

said master system monitors said security subsystem through said secure link by comparing the pseudo-attacks generated by said testing means to the detected attacks registered by said security subsytem.

9.   The network security system of Claim 8 wherein said master system is hierarchically independent from said security subsystem.

10.   The network security system of Claim 8 wherein said security subsystem is hierarchically subordinate to said master system.

11.   A method for monitoring the integrity of a security subsystem associated with a target network of computers and configured to detect attacks on said network of computers comprising:

establishing a secure link for the transfer of data between said security subsystem and a master system hierarchically independent from said security subsystem;

monitoring the status of said security subsystem through said secure link; and

registering information pertaining to the status of said security subsystem.

13

12.   The method for monitoring the integrity of a security system of Claim 11 including

the steps of:

        connecting said master system and said target network separately to an open network

of computers;

        generating at least one pseudo-attack in said master system, said pseudo attack being

detectable by said security subsystem;

        generating in said master system a list of expected responses to said at least one

pseudo-attack;

        delivering said at least on pseudo-attack over said open network to said target

network; and

        comparing the response of said security subsystem to said pseudo-attack to the list of
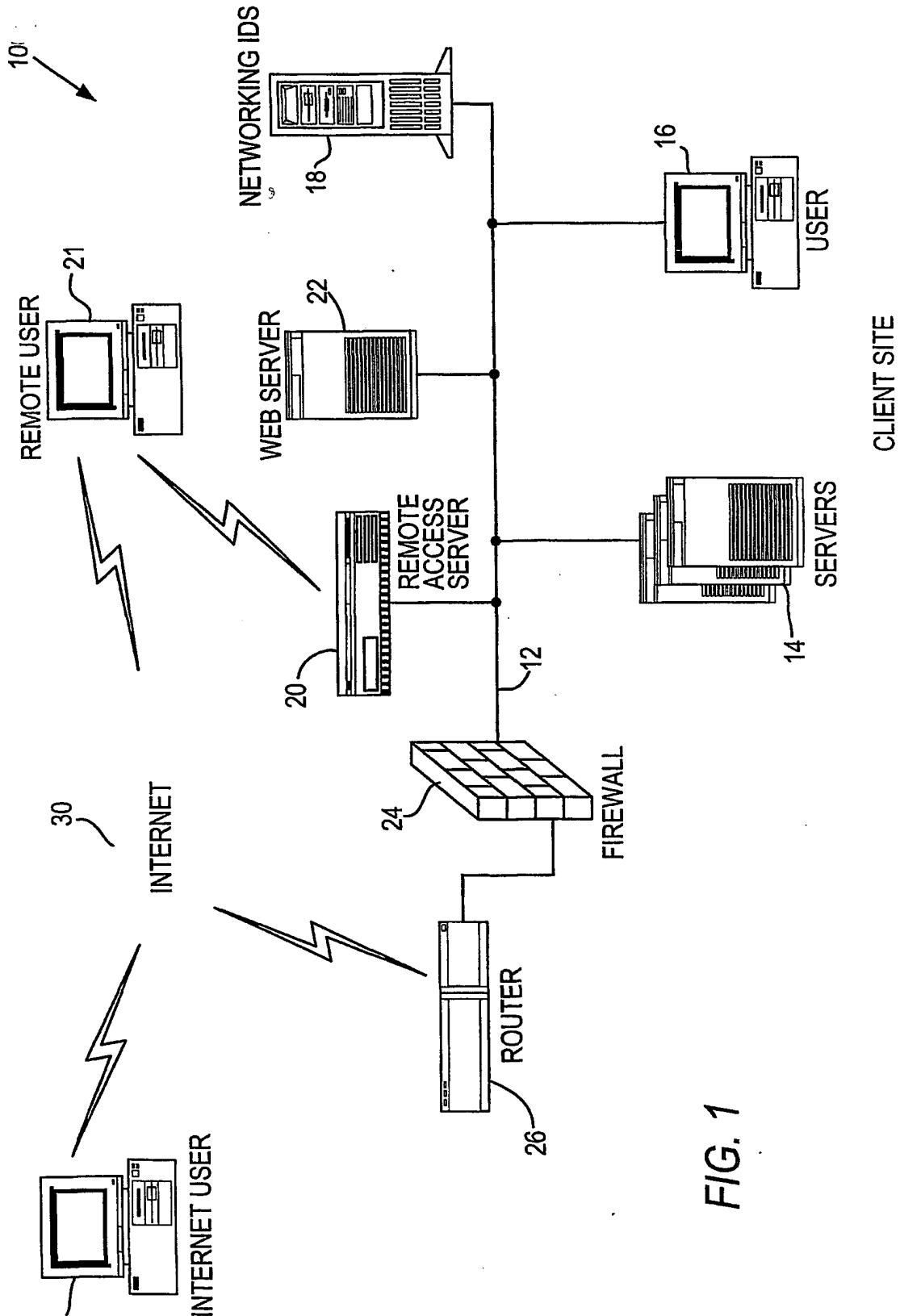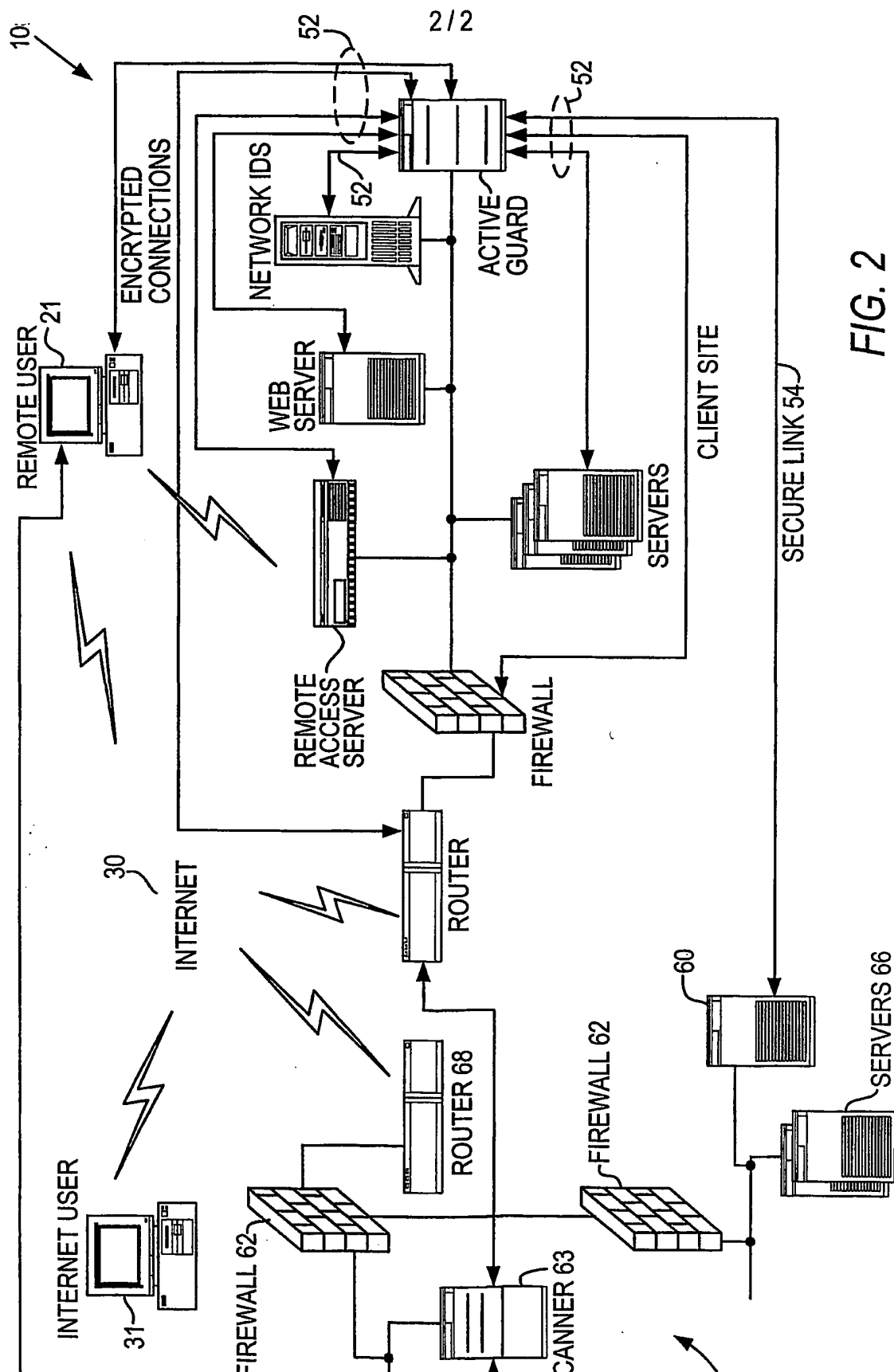
expected responses thereto.

1 / 2

NETWORKING IDS

18

REMOTE USER

21

WEB SERVER

22

REMOTE ACCESS SERVER

20

USER

16

SERVERS

14

12

FIREWALL

24

ROUTER

26

INTERNET

30

INTERNET USER

CLIENT SITE

10

FIG. 1

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/02218

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : HO4L 9/00
US CL : 713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/200,201; 380/2

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,088,804 A (HILL et al) 11 July 2000, column 4, lines 31-41; column 5, lines 7-15; column 8, lines 35-61	. 1, 3-7, 11
---		---------
Y		2, 8-10, 12
A	Anonymous, Security, December 1998, "Firewalls: Inside, outside and integrated"	1, 3-7, 11
A	Anonymous, PR Newswire, 29 June 1998, "Network Associates Redefines Network Intrusion Detection With CyberCop"	2, 8-10
X	Johnson, Johna Till, Data Communications, 21 November 1995, "Simulated attack for real network security", pages 31-32	1, 3-7, 11, 12
---		---------
Y		2, 8-10
X	US 5,961,644 A (KURTZBERG et al) 05 October 1999, column 3, lines 1-50	1, 3-7, 11
Y	Microsoft Press Computer Dictionary, Third Edition, Microsoft Press, 1997, page 258	12

☐ Further documents are listed in the continuation of Box C.   ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier application or patent published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 May 2002 (15.05.2002)	**18 JUN 2002**
.Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Gail Hayes *James R. Matthews* Telephone No. 703-305-1373

Form PCT/ISA/210 (second sheet) (July 1998)

Continuation of B. FIELDS SEARCHED Item 3:
EAST: master and subystem, master same subystem, master same slave, (simulat$ or generat$) adj attacks, master same slave, monitor same probe; PROQUEST: simulated attacks, networks, intrustion detection; IEEE XPLORE: simulated attacks, networks, intrusion detection